Eavesdropping without quantum memory

H. Bechmann-Pasquinucci

University of Pavia, Dipartimento di Fisica "A. Volta", via Bassi 6, I-27100 Pavia, Italy

UCCI.IT, *via Olmo 26, I-23888 Rovagnate, Italy*

March 31, 2005

Abstract

In quantum cryptography the optimal eavesdropping strategy requires that the eavesdropper uses quantum memories in order to optimize her information. What happens if the eavesdropper has no quantum memory? It is shown that the best strategy is actually to adopt the simple intercept/resend strategy.

1 Introduction

With the development of quantum information theory, traditional quantum state discrimination has, in many cases, been given a twist. It is no longer just the simple question of identifying one state drawn from a known set of states. Often there is additional information available after the interaction with the 'unknown' system or even after the measurement has been performed. For example, in the BB84 protocol [1] for quantum cryptography [2] the eavesdropper, Eve, knows that the quantum system is prepared with equal probability in a states belonging to a set of states made by two mutually unbiased bases. Moreover, she knows that after her eavesdropping, i.e. after the interaction with the 'unknown' quantum state, she will learn in which basis the system was originally prepared. She then uses this additional classical information, to gain more information about the initial state.

For the BB84 protocol, the optimal eavesdropping strategy [3], consists in intercepting the system prepared by Alice, attach an ancilla and let the combined system undergo a unitary interaction. After the interaction the original system is forwarded to Bob, whereas Eve keeps the ancilla. In this way she can transfer some of the information about the original state to her ancilla, with the cost of disturbing the original state and hence introduce errors on Bob's part. The more information

Eve transfers to her own system, the more she is disturbing the original system and the higher error rate she is introducing. In order for Eve to get the maximum information out of her ancilla, it is usually assumed that she does not measure her ancilla until after the public discussion between Alice and Bob. In this way she can use the knowledge that she gains by passively listening to the public discussion to select the measurement best suited for each ancilla. However, this requires that Eve is able to store her ancilla for a certain amount of time in a quantum memory. Here we ask the question, what happens if Eve does not have a quantum memory?

In this paper we consider the standard BB84 protocol [1] for qubits and discuss basically two different scenarios: the simple intercept/resend eavesdropping [4] and eavesdropping using an ancilla — but without a quantum memory. In both cases we consider a range of von Neumann measurements.

The scenario which is considered here is very simple, but the underlying question is both important and interesting because it concerns not only eavesdropping, but a much more general scenario: What happens when state discrimination is combined with additional classical information? What is the optimal measurement, when there later will be given additional classical information? These are questions which are interesting to consider in full generality. The study made in this paper should be considered only the beginning.

2 Intercept/resend eavesdropping

Consider the BB84 protocol for qubits, which uses two mutually unbiased bases for the secret key creation. We assume that Alice and Bob use the x and the y-basis, and use of the following definition of the states,

$$|\, x_\pm \,\rangle = \frac{1}{\sqrt{2}}(|\, 0 \,\rangle \pm |\, 1 \,\rangle) \quad \text{and} \quad |\, y_\pm \,\rangle = \frac{1}{\sqrt{2}}(|\, 0 \,\rangle \pm i|\, 1 \,\rangle) \tag{1}$$

here expressed in the computational basis $|\, 0 \,\rangle$ and $|\, 1 \,\rangle$.

First we will consider intercept/resend eavesdropping, which historically also was the first eavesdropping strategy to be considered. This strategy requires no quantum memories, and it is reviewed in order to compare with the optimal eavesdropping strategy *without* quantum memory. It consists very simply in Eve intercepting the qubit prepared by Alice while in transit to Bob, she then estimates the state of the qubit by means of a measurement, and prepares a new qubit in the state that she found and sends it to Bob. We assume that Eve performs a von Neumann measurement lying in the xy-plane[1]. It is possible to consider all measurement

[1] In higher dimension it will be necessary to consider POVMs [5]

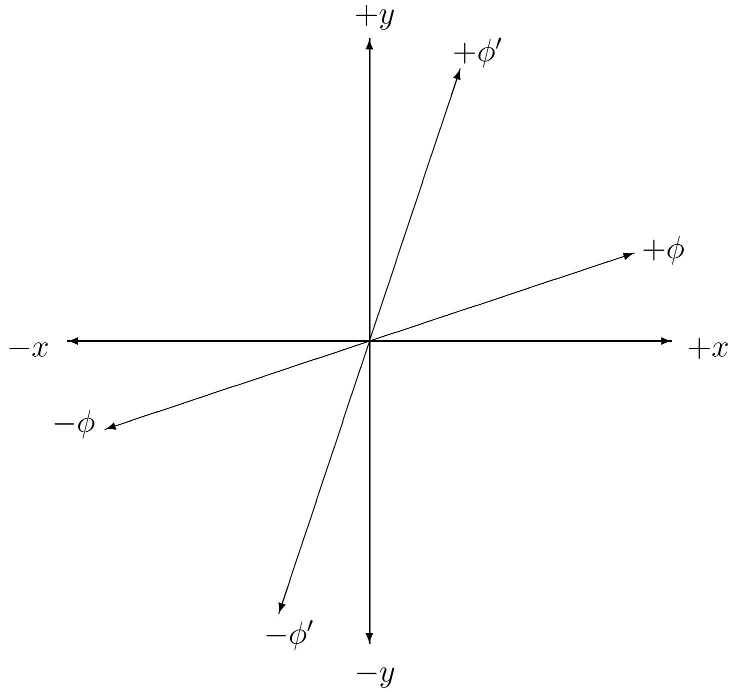

Figure 1: Here is shown the x and the y basis and the two measurement bases used by Eve, ϕ and ϕ'. Notice that the states are drawn on the equator of the Poincare sphere.

strategies of this kind in one go, by parameterizing the measurement as follows:

$$|+\phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\phi}|1\rangle) \quad \text{and} \quad |-\phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - e^{i\phi}|1\rangle), \tag{2}$$

where $\phi \in [0, \pi/4]$. Since this measurement is not symmetric with respect to the two bases, Eve will have different fidelities and disturbances in the two bases, moreover she will also introduce different error rates in the two bases. However, it is easy to restore the symmetry by letting Eve choose at random between two different measurements: namely the ϕ-measurement and the measurement which corresponds to $\phi' = \pi/2 - \phi$ (see fig. 1). Notice that this symmetrization doesn't change Eve's average information. When performing the ϕ or ϕ' measurement, Eve will obtain the following fidelities and disturbances in the two bases:

$$\begin{aligned} F^x_{E,\phi} = F^y_{E,\phi'} = \frac{1}{2}(1+\cos\phi) \quad &, \quad D^x_{E,\phi} = D^y_{E,\phi'} = \frac{1}{2}(1-\cos\phi) \\ F^y_{E,\phi} = F^x_{E,\phi'} = \frac{1}{2}(1+\sin\phi) \quad &, \quad D^y_{E,\phi} = D^x_{E,\phi'} = \frac{1}{2}(1-\sin\phi) \end{aligned} \tag{3}$$

Where as usual we have $F^i_{E,\phi} + D^i_{E,\phi} = 1$.

Independently of whether Eve measures in the ϕ or the ϕ'-basis, half of the times Alice has prepared the qubit in the x-basis, and half of the time she has prepared the qubit in the y-basis. Eve obtains the following amount of Shannon information [6], respectively

$$\begin{aligned} I^x_{E,\phi} = I^y_{E,\phi'} = 1 + F^x_{E,\phi} \log F^x_{E,\phi} + D^x_{E,\phi} \log D^x_{E,\phi} \\ I^y_{E,\phi} = I^x_{E,\phi'} = 1 + F^y_{E,\phi} \log F^y_{E,\phi} + D^y_{E,\phi} \log D^y_{E,\phi}. \end{aligned} \tag{4}$$

This means that Eve's average information is

$$I_E = \frac{1}{4}(I^x_{E,\phi} + I^y_{E,\phi} + I^x_{E,\phi'} + I^y_{E,\phi'}). \tag{5}$$

After her measurement Eve has to prepare a new qubit and send it to Bob. However, at this point in the protocol Eve doesn't know in which basis the original qubit was prepared. We consider the usual case where she prepares the same state that she found by her measurement and sends that to Bob.

Assuming that Eve measures in the ϕ basis, then the fidelity and disturbance which Bob finds, can be obtained by the following argument: with probability $F^i_{E,\phi}$, $i = x, y$, Eve will find the correct *guess* state and send it to Bob; where correct *guess* state means that if Alice sent a + state then Eve will identify the state as the $+\phi$, etc. Assuming that Bob measures in the same basis as Alice, he will then have probability $F^i_{E,\phi}$ of obtaining the correct state. Whereas with probability $D^i_{E,\phi}$ Eve finds the wrong *guess* state and hence sends the wrong state to Bob. However, if Bob makes the wrong identification of the wrong state, he will actually obtain the correct state; this will happen with probability $D^i_{E,\phi}$. So in total Bob's probability for getting the correct state is:

$$\begin{aligned} F^x_{B,\phi} = (F^x_{E,\phi})^2 + (D^x_{E,\phi})^2 = \frac{1}{2} + \frac{\cos^2\phi}{2} \quad (= F^y_{B,\phi'}) \\ F^y_{B,\phi} = (F^y_{E,\phi})^2 + (D^y_{E,\phi})^2 = \frac{1}{2} + \frac{\sin^2\phi}{2} \quad (= F^x_{B,\phi'}) \end{aligned} \tag{6}$$

As for Eve, due to symmetry we have $F^x_{B,\phi} = F^y_{B,\phi'}$ and $F^y_{B,\phi} = F^x_{B,\phi'}$.

Making use of the expressions of Eve's fidelity and disturbance, one finds that Bob's overall fidelity $F_{B,\phi} = \frac{1}{2}(F^x_{B,\phi} + F^y_{B,\phi}) = 3/4$, and disturbance $D_{B,\phi} = 1 - F_{B,\phi} = 1/4$ is independent of the measurement performed by Eve. However, if Eve doesn't alternate between the two bases ϕ and ϕ', Bob will find different fidelities and disturbances in his two bases, see eq.(6).

There are a couple of special values of ϕ which are worth considering more explicitly, namely the case $\phi = 0$ and $\phi = \pi/4$: The case where $\phi = 0$ and hence $\phi' = \pi/2$, corresponds the the situation where Eve is measuring at random in the

x and the y-basis, hence using the same bases as Alice and Bob. The information that Eve obtains in this situation is so-called deterministic information, becuase when the three of them use the same basis, Eve knows the secret bit, whereas if she measures in the wrong basis she will no nothing about the bit value. On average Eve gains 1/2 a bit of information.

In the case where $\phi = \pi/4$, we have a very special situation. In this case the ϕ-measurement and the ϕ'-measurement coincides and Eve no longer needs to choose at random between two measurements, since this single measurement treats the two bases symmetrically. This particular attack in known as the intercept/resend attack in the intermediate basis [7]. It can be shown that that this measurement optimizes Eve's probability of guessing the state correctly *independently* of the basis. Which means that Eve obtains the same amount of information on each single bit. However, her information is no longer deterministic, but probabilistic, which means that she knows she bit with a certain probability (different from 1). Even if this measurement strategy gives Eve less information ($I_E \approx 0.39$), than measuring in the same basis as Alice and Bob, it is an advantage for Eve, when it is taken into account that Alice and Bob later will go through classical error correction and privacy amplification [4]. This is due to the fact that probabilistic information is more robust during this process than deterministic information.

As a curious point should be mention that the states corresponding to the intermediate states, also play an optimal role in the game of quantum state targeting[8, 9] and Bell inequalities [10].

In order to compare with the results in the next section it is useful to display the information that Eve obtains as a function of the disturbance that she introduces. Eve can lower the disturbance by eavesdropping only on a fraction $f \in [0, 1]$ of the transmitted qubits, where $f = 0$ corresponds to no eavesdropping and $f = 1$ to eavesdropping on all qubits. Assuming that eavesdropping is the only cause of errors, then the disturbance that Alice and Bob will find if Eve only eavesdrop on a fraction of the qubits is $D_B = f \cdot D_{B,*} = \frac{f}{4}$, since $D_{B,\phi} = D_{B,\phi'} = 1/4$. Similarly, Eve's average information becomes $f \cdot I_E$. It is possible to express Eve's information in terms of the disturbance that she creates, since $f = 4D_B$, which means $I_E(D_B) = 4D_B I_E$. The corresponding information curves are displayed in figure 2. Notice that the information curves for intercept/resend eavesdropping are only defined up til the disturbance $D_B = 1/4$, since this is the disturbance which Eve would introduce if she would eavesdrop on each single qubit. Furthermore it should be kept in mind that these information curves corresponds to the average information on the full key, since Eve obviously has no information when she doesn't eavesdrop.

Since $\phi \in [0, \pi/4]$, the two special cases considered above correspond to the end points of the interval, changing the parameter ϕ will therefore smoothly change the information curve from $I_{E,0} \equiv$ I_E_irxy to $I_{E,\pi/4} \equiv$ I_E_irint, see Fig.2.

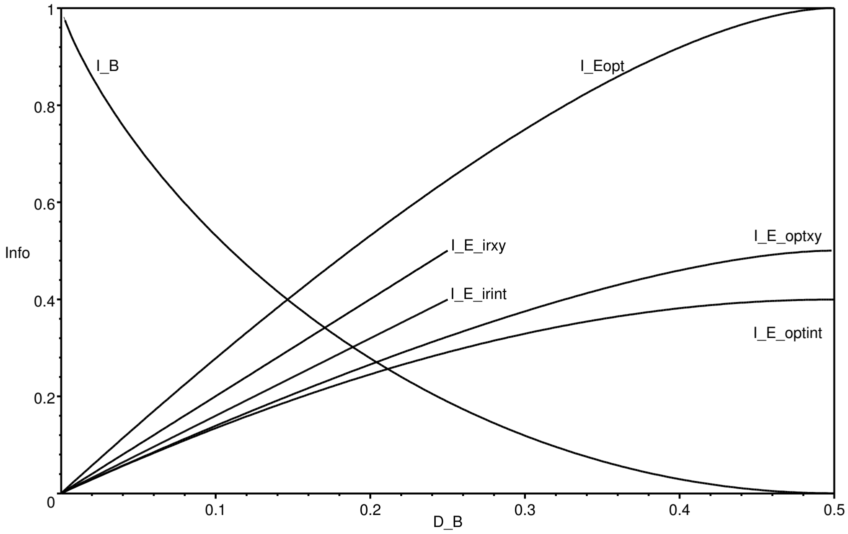

Figure 2: The information curves as a function of the disturbance detected by Bob: I_B $\equiv$ Bob's information. For Eve: I_Eopt $\equiv$ optimal information *with* quantum memory, I_E_irxy $\equiv$ intercept/resend measurement in the x, y bases, I_E_irint $\equiv$ intercept/resend measurement in intermediate basis, I_E_optxy $\equiv$ optimal eavesdropping *without* quantum memory, measurement in the x, y bases, I_E_optint $\equiv$ optimal eavesdropping *without* quantum memory, measurement in the intermediate basis. Notice that by changing $\phi \in [0, \pi/4]$, the information curve smoothly goes from I_E_$*$xy to I_E_$*$int (see also Fig.3).

3 Optimal eavesdropping

The optimal eavesdropping strategy consists in Eve letting an ancilla undergo a unitary interaction with the qubit prepared by Alice, after which she sends on the (now disturbed) qubit to Bob and keeps her ancilla. Eve usually stores her ancilla in a quantum memory and only performs a measurement on it after she has learnt from the public discussion between Alice and Bob in which basis the original qubit was prepared. In order to optimize her information Eve has to measure her ancilla in same the basis as the qubit was originally prepared.

When expressed in the computational basis, i.e. the z-basis, the optimal eavesdropping strategy can be written on the following simple, but asymmetric form

$$\begin{aligned} |\,0\,\rangle|\,0\,\rangle &\xrightarrow{\mathbf{U}} |\,00\,\rangle \\ |\,1\,\rangle|\,0\,\rangle &\xrightarrow{\mathbf{U}} \cos\alpha|\,10\,\rangle + \sin\alpha|\,01\,\rangle \end{aligned} \tag{7}$$

where the lefthandside indicates the state before the interaction and the righthandside the state after the interaction of the qubit sent by Alice and the Eve's ancilla.

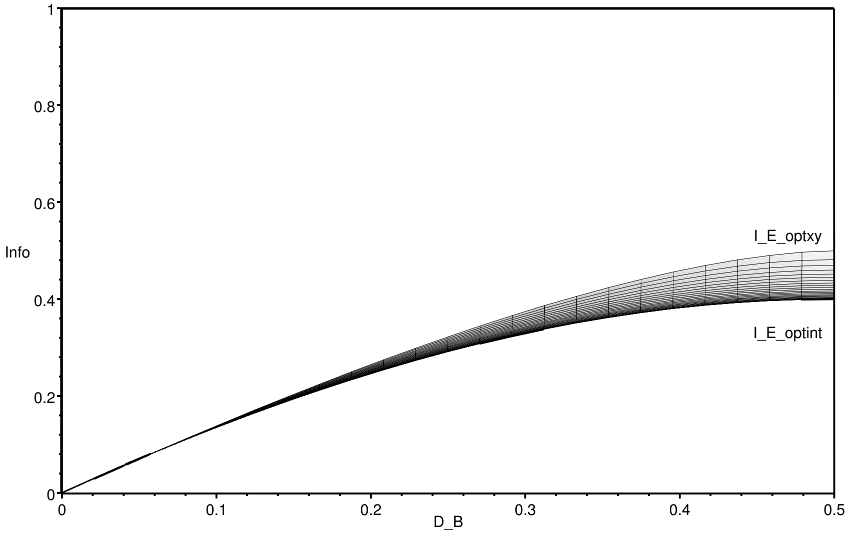

Figure 3: The bottom curve corresponds to measuring in the intermediate basis ($\phi = \pi/4$) and the top curve corresponds to measuring in the x or y basis.

The fidelities of Bob and Eve are $F_B = (1 + \cos\alpha)/2$, and $F_E = (1 + \sin\alpha)/2$, respectively. The disturbance is $D_i = 1 - F_i$, where $i = \{B, E\}$.

It should be emphasized that with respect to the x and y-basis the eavesdropping strategy is symmetric and the fidelities are therefore also the same for the two basis. The information curves for Bob and Eve $I_i = 1 + D_i \log_2 D_i + (1 - D_i)\log_2(1 - D_i)$, where $i = \{B, E\}$ are shown in figure 2, where Eve's disturbance has been expressed in terms of Bob's disturbance D_B, i.e. $D_E(D_B)$. However, it should be remembered, that in order for Eve to optimize her fidelity and her information Eve has to perform her measurement *after* the public discussion between Alice and Bob, which means storing her qubit in a quantum memory.

We will now consider a situation which is less ideal for Eve — but much more realistic as of today — namely where Eve has no possibility of storing her ancilla in a quantum memory and therefore has to make a measurement right a way. As in the case of intercept/resend eavesdropping, Eve will still listen to the public discussion between Alice and Bob, because even if the information about the original basis preparation of the qubit arrives *after* she has performed her measurement she can still use the information to make an interpretation of her measurement result and obtain more information.

Consider again the situation where Eve measures with equal probability in either the ϕ or the ϕ' basis. Then, if she has let her ancilla undergo the interaction described in eq.(7), she will have the following measurement fidelity and disturbance:

$$\begin{aligned} F^x_{E,\phi} &= \frac{1}{2}(1+\cos\phi\sin\alpha) \quad , \quad D^x_{E,\phi} = \frac{1}{2}(1-\cos\phi\sin\alpha) \\ F^y_{E,\phi} &= \frac{1}{2}(1+\sin\phi\sin\alpha) \quad , \quad D^y_{E,\phi} = \frac{1}{2}(1-\sin\phi\sin\alpha) \end{aligned} \tag{8}$$

Where as usual we have $F^i_{E,\phi} + D^i_{E,\phi} = 1$, and again due to symmetry (see figure 1) $D^x_{E,\phi} = D^y_{E,\phi'}$ and $D^y_{E,\phi} = D^x_{E,\phi'}$. Bob's fidelity and disturbance do not change.

Based on the obtained fidelity and disturbance, the information can be computed $I_E(D_B) = \frac{1}{4}(I(D^x_\phi) + I(D^y_\phi) + I(D^x_{\phi'}) + I(D^y_{\phi'}))$. The resulting information curves in the range $\phi \in [0, \pi/4]$ are shown in Fig. 2 and 3.

4 Conclusion

When looking at the curves in figure 2, one would conclude that if Eve does not possess a quantum memory, then the best that she can do is to resolve to intercept/resend eavesdropping. However, one should be careful about drawing conclusions from figure 2 alone. It should be remembered that in order to be able to draw the curve for the intercept/resend eavesdropping it was assumed that Eve was intercepting only a fraction of the qubits, hence the information that Eve possess in this case should be viewed as an average information on the full key. In the intercept/resend strategy Eve's handlebar for controlling the disturbance D_B is by intercepting only a fraction of the qubits, naturally she has no information on the qubits she doesn't eavesdrop on, whereas on the qubits that she eavesdrop she will actually have a lot of information. On the other hand, when Eve uses an ancilla, she is interacting with each single qubit and the disturbance D_B is determined by the strength of her interaction (which is assumed to be the same for all the qubits).

However, a couple of conclusions can be made: when Eve performs intercept/ resend eavesdropping on all the transmitted qubits she introduces a disturbance $D_B = 1/4$ independently of the measurement she has chosen. Considering now the eavesdropping strategy with the ancilla: in order to get the same amount of information as for the intercept/resent eavesdropping intercepting all qubits, Eve will introduce a disturbance which is twice as big, namely 1/2. At first it may seem curious that Eve by performing two so different eavesdropping strategies will end up with the same amount of information. However, is should be remembered that the optimal eavesdropping strategy is symmetric with respect to Eve and Bob and that when the disturbance is $D_B = 1/2$ it corresponds to interchanging Eve and Bob. This basically means that Eve keeps the qubit sent by Alice and prepares a new qubit at random in one of the four states and sends it to Bob. Which makes it immediately clear that in this situation Eve's information corresponds to the information she would have gotten in the intercept/resend eavesdropping — but since she sends Bob one of the four states at random, she obviously introduce a much higher disturbance.

As of today, the scenario we have considered here is actually quite realistic, since there is still a long way before having quantum memories which will allow an eavesdropper to store her ancilla for the required amount of time. The eavesdropper will then be forced to perform her measurement immediately, and as we have just seen in this situation a simple intercept/resend eavesdropping strategy is actually what will optimize her information.

Acknowledgment

This work has been supported by EC under project SECOQC (contract n. IST-2003-506813)

References

[1] C. H. Bennett, G. Brassard, in it Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India (IEEE, New York, 1984), p. 175.

[2] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, *Rev. Mod. Phys.* **74**, 145 (2002)

[3] C-S. Niu, R. B. Griffiths, *Phys. Rev. A* **60**, 2764 (1999)

[4] C. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin, *J. Cryptology* **5**, 3 (1992)

[5] D. Kaszalikowski, A. Gopinathan, Y. C. Liang, L. C. Kwek, B.-G. Englert, *Phys. Rev. A* **70**, 0032306 (2004)

[6] T. Cover, J. Thomas, *Elements of Information Theory*, Wiley Series in Telecommunications (Wiley, New York, 1991)

[7] C. Bennett, G. Brassard, S. Breidbart, S. Wiesner, *Advances in Cryptology: Proceedings of Crypt'82*, August 1982, Plenum, New York, p. 267

[8] T. Rudolph, R. Spekkens, *Phys. Rev. A* **70**, 052306 (2004)

[9] H. Bechmann-Pasquinucci, quant-ph/0406106 (accepted for publication in Found.Phys. special issue: Festschrift for Asher Peres)

[10] H. Bechmann-Pasquinucci, N. Gisin, *QIC* **3** 157-164 (2003)